

An ISO/IEC 15408 based Functional Package

**Security Functional Package for Systems Transmitting
Sensitive HCFA data (STS-HCFA)
----- (Draft for Version 1.0 – 8/3/99) -----**

Sponsored by

**Advanced Technology Program (ATP)
National Institute of Technology (NIST)**

&

**National Information Assurance Partnership (NIAP)
A Joint Program of
National Institute of Technology (NIST) &
National Security Agency (NSA)**

Developed by

Ramaswamy Chandramouli (NIST)

Reviewed by

TABLE OF CONTENTS

SECTION	PAGE
1. Introduction	3
2. General Characteristics of STS-HCFA Systems	6
3. Security Environment	7
4. Security Objectives for STS-HCFA	10
5. STS-HCFA Security Functional Requirements	11
6. Rationale for choice of ISO 15408 Security Functional Classes	16
Appendix A	18
Glossary of Terms	19
Bibliography	20

Security Functional Package for Systems Transmitting Sensitive HCFA data (STS-HCFA)

1. Introduction

The Healthcare Financing Agency (HCFA) is an agency under the Department of Health and Human Services (HHS) that administers medicare and medicaid programs. In November of 1998, HCFA issued an internet security policy document [refer HISP]. This document provides guidelines for the security and appropriate use of the internet to transmit HCFA Privacy Act-protected and other sensitive HCFA information.

The issuance of Internet security policy document (hereafter referred to as HISP in the rest of this document) by HCFA has two important implications:

- (1) It provides unprecedented opportunities for interaction and data sharing among all players dealing with HCFA information resource – health care providers providing Medicaid & Medicare services, HCFA contractors, HCFA components, state agencies acting as HCFA, Medicare and Medicaid beneficiaries and researchers.
- (2) It requires that systems or processes which use the Internet, or interface with the Internet, to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information (these two categories of information are referred to as just HCFA-sensitive in the rest of the document) including Virtual Private Network (VPN) and tunneling implementations over the Internet.

The second implication in turn requires that the following two processes be set in motion.

- (1) First it requires that product developers and system integrators who want to develop information systems to transmit HCFA-information over the internet must incorporate security functionality into their systems that comply with HCFA Internet Security Policy.
- (2) Secondly, the accreditation/certification bodies should have a means of gaining assurance that a system developed by a particular vendor for this purpose (i.e., use of Internet for uploading and downloading HCFA Privacy-act protected information) does indeed comply with the HCFA Internet Security Policy requirements.

The above two processes will be facilitated if the following are available:
(we refer to these as PSF1, PSF2 & PSF3 where the abbreviation PSF stands for Process Support Facilities)

- (1) PSF1: There exists a means for personnel involved in the procurement of systems dealing with transmission of HCFA data to articulate the security requirements (necessitated by HCFA Internet Security Policy) in a standardized , unambiguous way .
- (2) PSF2: There exists a means for system vendors to claim compliance with those requirements (stated through PSF1) by describing the security mechanisms/features in their products/systems.
- (3) PSF3: Either through PSF1 and/or PSF2 or through separate means, benchmarks should be available for IT security evaluators for ensuring compliance to HCFA Internet Security Policy.

1.1 ISO/IEC 15408 Criteria for Evaluation of IT Security

The constructs available in the ISO/IEC specification 15408 provides the three facilities (PSF1, PSF2 & PSF3) needed for supporting the process of mapping HCFA Internet Security Policy requirements to security functional requirements and providing benchmarks for evaluating systems that have implemented these security functional requirements. Part 1 of ISO/IEC 15408 [refer to ISO/IEC 15408-1] provides the specification for constructs called the **Protection Profile** (hereafter abbreviated as PP). and the **Security Target** (hereafter abbreviated as ST).

The *Protection Profile (PP)* is a document intended for the user community to express their security functional requirements and security assurance requirements. To express these security functional requirements (SFR) and security assurance requirements (SAR) in an unambiguous way, the ISO/IEC 15408 provides a pre-defined catalog of these requirements ([refer to ISO/IEC 15408-2] for the catalog of Security Functional Requirements and [ISO/IEC 15408-3] for the catalog of Security Assurance Requirements). To provide a complete environment and context for these functional and assurance requirements ,the PP document also contains sections for (a) Description of TOE (abbreviation for Target of Evaluation to denote the IT system under consideration) (b) Security Environment for the TOE (expressed in terms of Threats, Organizational Policies and Usage Assumptions).

The *Security Target (ST)* is a document intended for vendors to state the security functionality provided in their product that meets the security functional requirements stated in a Protection Profile (PP). Hence it contains all the sections in a PP in addition to a section called “TOE Summary Specification” where the vendor describes the security mechanisms built into their particular product.

The *security functional requirements* components from the ISO/IEC 15408’s pre-defined catalog (which are used in both PP and ST) are flexible enough to capture any security policy requirements and translate them into security functional requirements in a standard format since they contain pre-defined operators to extend and/or modify the pre-defined components.

The *security assurance requirements* components in ISO/IEC 15408 are organized in terms of seven assurance levels (EAL1 thru EAL7) to enable the user community to state the degree of security assurance required and/or the vendor to state the degree of assurance that he/she can offer. Based on this stated assurance level and the security assurance components that pertain to that level, the system evaluators can conduct their evaluation of the system for conformance to the stated/claimed security functional requirements by the vendors.

Protection Profiles (and Security Targets) are developed for a particular product (e.g., DBMS, Operating System) or a specific application system that supports a well-defined business process. With reference to the context of this document, an example of an application system may be a Billing System in a Hospital that treats medicare/medicaid patients and hence generates and transmits billing claims information (HCFA-sensitive information) to an HCFA agency.

The HCFA Internet Security Policy (HISP) is intended to cover security requirements for any type of system that provides the following functionality - generate, transmit and/or receive HCFA-sensitive information. Hence HISP is not meant for any particular application system but to a family of application systems that provides the above stated functionality. In addition, each of these systems in the family may have numerous other features and functions, which in turn may bring in additional security requirements as well. Hence it is difficult to define the complete security context that is applicable across the board to all systems transmitting/receiving HCFA data. Consequently, the ISO/IEC 15408 PP or ST is not a suitable framework for capturing HCFA Internet Security Policy Requirements since these constructs (i.e., PPs and STs) are meant for a specific application system whose security perimeter (complete security context) is known.

However the HISP requirements can be mapped to a set of pre-defined security functional components in ISO/IEC 15408. It is also possible to associate objectives with these security functional requirements and also state the general security environment where such policies are applicable as well. Hence we see that we can map HISP requirements to all sections of a ISO/IEC 15408 protection profile except for the section dealing with security assurance components (since that requires the complete system security perimeter to be known). The document that results from such a mapping thus provides a means for aggregating ISO/IEC 15408 security functional requirements pertaining to a given organizational policy and is called a “Functional Package” since it provides a “ready to use” package of ISO/IEC 15408 security functional requirements (along with elements of security environment) that has resulted from the policy.

This document is the “Functional Package” (FP) meant for aggregating ISO/IEC 15408 security functional requirements pertaining to HCFA Internet Security Policy. This functional package contains the following information:

- (a) generic characteristics of systems that transmit/receive HCFA-sensitive data (called by the term TOE –targets of evaluation) for which this FP is written (Section 2).

- (b) the security environment in which these systems operate – described in terms of threats, security policies and usage assumptions (Section 3)
- (c) the overall security objectives needed for these systems (Section 4) and
- (d) the set of security functional requirements components (ISO/IEC 15408) needed to meet the stated security objectives (Section 5).

In addition, there is a section (Section 6) that provides the rationale for selection of the security functional components from ISO/IEC 15408 that is included in this Functional Package.

1.2 Intended use for this Functional Package

This Functional Package deals with security requirements needed for secure transmission (preserving both the confidentiality and integrity) of HCFA sensitive data through the public Internet as well as proper identification & authentication of the parties involved in this transmission. As already stated, the computing systems involved in generating and/or receiving these transmissions may have other functional capabilities (along with supporting data stores) which may require their own set of security requirements especially those pertaining to stored data protection and access to various menu functions etc., These requirements are outside the scope of this Functional Package. However a developer of a PP for a specific application system (that processes and transmits HCFA sensitive data – for e.g., a healthcare claims billing system) can readily use this Functional Package to gather the comprehensive set of security functional requirements needed for the entire system instead of developing each requirement for the system from the basic component provided in ISO/IEC 15408.

2. General Characteristics of STS-HCFA systems

The HCFA Internet Security Policy (HISP) covers all systems and processes which use the Internet, or interface with the Internet, to transmit HCFA Privacy Act-protected and/or other sensitive HCFA information, including Virtual Private Network (VPN) and tunneling implementations over the Internet. There may be many different types of application systems processing and transmitting the above category of HCFA data. The ISO 15408 uses the term TOE (Target of Evaluation) to refer to an application system. In this functional package we use the term STS-HCFA (which stands for Systems Transmitting Sensitive HCFA data) to refer to the entire family of such systems.

Some of the examples in the family of application systems referred to above are:

- (a) Systems that generate and receive payment and billing information (say in ANSI ASC X12 837 COB format) between payers of Medicare healthcare service with different payment responsibilities.
- (b) Systems that generate messages containing health care claim billing information, encounter information, or both (say in ANSI ASC X12 837 format), from providers of

Medicare health care services to payers of health care, either directly or via intermediary billers and claim clearinghouses.

(c) Systems that generate messages pertaining to enquiry and response re: Medicare Eligibility (say ANSI ASC X12 270 format (for Health Care Eligibility/Benefit Inquiry) and the ANSI ASC X12 271 format (for Health Care Eligibility/Benefit Information).

(d) Systems that generate messages pertaining to healthcare claim payment/advice (say in ANSI ASC X12 835 format).

From the above examples we can draw up the following *general characteristics of STS-HCFA systems* in terms of their functionality:

- (a) They extract HCFA-sensitive data using one or more interfaces and convert them into formatted messages (corresponding to formats in applicable EDI forms) and transmit them using standard communication protocols through the medium of public Internet.
- (b) They may transmit files containing HCFA-sensitive data as electronic mail attachments.

3 Security Environment

3.1 Threats

3.1.1 IT Assets

The IT assets requiring protection comprise the messages/transactions containing HCFA privacy act protected information in transit through the Internet. The confidentiality, integrity or availability of this information could be compromised.

3.1.2 Threat Agents

The threat agents could be:

- (a) Outsiders: Persons who are not authorized to transmit or receive HCFA privacy-act protected information. In addition, this category includes persons who view or modify HCFA information in transit through the network.
- (b) System Users: Persons who are authorized to use the communication interfaces of STS-HCFA to generate or receive HCFA information. Administrators who set configuration parameters for network security devices like firewalls, VPN software. Administrators who set up and maintain security related data like authentication data, authorization data, audit data etc.,
- (c) External Events: Interruptions to operations or compromise of security arising from failures of devices (hardware, storage media etc.,) which either perform security

functions like encryption or contain security related data like digital certificates, authentication data, authorization data, audit data etc.,

3.1.3 Forms of Attack

There are two forms of attack that might be carried out.

- (a) Unauthorized access to interfaces which receive or transmit HCFA information.
- (b) Impersonation

3.1.4 Threats countered by TOE (STS-HCFA) and its IT environment

- (a) T.SNIFF - IP Packet Sniffing: Sensitive data contained within an IP packet carrying a HCFA transaction could be viewed by unauthorized persons using techniques ranging from shoulder surfing to using sniffers to perform wire-tapping.
- (b) T.SPOOF - IP Spoofing: Since IP addresses are not physically bound to machines (like NICs in a LAN environment), a machine can claim to be associated with an IP address not assigned to it.
- (c) T.ENTRY – An unauthorized user may gain entry into STS-HCFA and either transmit or receive HCFA-sensitive information
- (d) T.INTEGRITY – HCFA-sensitive data transmitted over an internet circuit may be tampered with affecting the integrity of the data.

3.1.5 Threats countered by Operating Environment

- (a) T.FW_CONFIG (Badly configured firewall): Firewalls act as the logical filter for information/transactions flowing out and flowing into the network. Hence it is considered a trusted system component. Any misconfiguration can result in illegal HCFA information outflows/ inflows.

3.2 Organizational Security Policy

- (a) P. SENSITIVE - The following categories of information must be protected while transmitted over the Internet. They are:
 - (i) All individually identifiable data held in systems of records – these include automated systems of records subject to Privacy Act of 1974 , which contain information that meets the qualifications for Exemption 6 of the Freedom of Information Act.
 - (ii) Payment information that is used to authorize or make cash payments to individuals or organizations.

- (iii) Computerized correspondence and documents relating to HCFA transactions that are considered highly sensitive and/or critical to an organization and which must be protected from unauthorized alteration and/or premature disclosure.
- (b) P.SCOPE - The protection policy covers all systems that collect, maintain and disseminate sensitive HCFA data and employed by HCFA's contractors, state agencies (acting as HCFA agents) and any other entity that has been authorized to access to HCFA information. These include all forms of message handling systems including electronic mail systems and EDI based systems.
- (c) P.AUTHENTICATE – Systems transmitting & receiving HCFA-sensitive data should be mutually authenticated using strong forms of authentication like digital certificates, symmetric “private keys” or smart tokens.
- (d) P.CHANNEL – A secure channel should be set up between users and application systems using SSL V3.0 mechanisms. Also a secure channel for e-mail messages containing HCFA-sensitive information should be set up using S/MIME 2.0 standards.
- (e) P.ENCRYPT – All HCFA-sensitive data transmitted over public Internet must be encrypted using either hardware-based or software-based encryption devices to protect the confidentiality of the information.
- (f) P.ACCOUNTABILITY – Every user (normal users as well as administrators) shall be held accountable for any action performed on STS-HCFA system especially dealing with transmission and receipt of HCFA transactions/messages.
- (g) P.SECMGT – There should management mechanisms in place to manage data used for performing security relevant functions. Examples of such data are passwords, public/private key pairs, symmetric keys etc., Also there should be effective mechanisms to manage the security administrative functions.

3.3 Security Usage Assumptions

This section describes the security aspects of the environment in which the STS_HCFA will be, or is intended to be used. This includes information about the physical, personnel and connectivity aspects of the environment.

3.3.1 Connectivity Assumptions

- (a) A. CONNECT - STS-HCFA performs all security related tasks (like encryption and digital signatures) before sending packets over the public Internet. Remote access to

STS-HCFA is permitted after being suitably authenticated using a digital certificate or a smart token.

- (b) A.PEER – All systems to which STS-HCFA transmits data are authenticated prior to each transmission. Similarly the identities of all systems from which STS-HCFA receives data are checked and the integrity of data transmission verified before the received HCFA transaction is stored in STS-HCFA data store.

3.3.2 Physical Assumptions

- (a) A.LOCATE: The processing resources of STS-HCFA (except possibly remote access facilities) are located within controlled access facilities which are “reasonably safe” from typical natural hazards as well as unauthorized physical access. The safety aspect can be ensured by housing the STS-HCFA resources in a facility that shall conform to the established local building standards including installation of various types of alarms and an administrative mechanism to promptly respond to such alarms when activated. Unauthorized physical access can be enforced by restricting entry using electronic locks trained guards & ID cards.
- (b) A.PROTECT: The hardware and software critical to security policy enforcement (e.g., - encryption devices – in case of hardware encryption, firewalls, VPN hardware and software, storage devices containing security administration data like audit logs, authorization data, authentication data, digital certificates etc, software modules that perform security functions like encryption, digital signatures etc) is physically protected from unauthorized modification by potentially hostile outsiders.

3.3.3 Personnel Assumptions

- (a) A. TRUST – There will one or more competent individuals assigned to administer STS-HCFA and ensure its secure operation. These administrators are assigned privileges commensurate with their skill level and degree of trust.
- (b) A.TRAINING - There should be a minimum level of security awareness for all users of STS-HCFA. In addition , individuals deemed critical for secure operations (e.g., system administrators, security officers etc) shall receive additional training in secure operations, procedures etc.,
- (c) A.SYSAUDIT – Internal and/or external system auditors shall be available to conduct periodic security audit (reviews).

4. Security Objectives for STS-HCFA

The security objectives for STS-HCFA have been formulated to counter *the identified threats in section 3.1.4* and support the *policy components listed in section 3.2* which reflect the policy requirements stated in the HCFA Internet Security Policy.

O.CHANNEL – STS-HCFA shall establish a secure channel between systems transmitting HCFA-sensitive data.

O.AUTHENTICATE – STS-HCFA shall set up strong authentication mechanisms between transmitter and receiver of HCFA-sensitive information prior to start of actual data transmission.

O.ENCRYPT – STS-HCFA shall encrypt all data that is being transmitted over the public Internet in order to preserve the confidentiality of HCFA-sensitive data

O.INTEGRITY – STS-HCFA shall protect the integrity of the HCFA-sensitive data transmitted over public Internet by means such as checksum or digital signatures

O.AUDIT – STS-HCFA shall generate audit records for all security relevant events taking place between transmitter and receiver of HCFA-sensitive data in order to hold users of these systems accountable for their actions

O.SECADMIN – STS-HCFA shall provide administrative functions for secure management of all security relevant functions and their associated data.

5. STS-HCFA Security Functional Requirements

This section contains security functional requirements that must be satisfied by STS-HCFA in order that it satisfies the policy requirements in the HCFA Internet Security Policy.

The security functional requirements components stated in this section are drawn from part 2 of ISO 15408 security criteria. The ISO 15408 security functional components provide operations like **Iteration, Assignment, Selection and Refinement** which provide extensibility to the pre-defined components. These operations are used to tailor the security requirements (functional) to the level of detail necessary to meet the security objectives (and by implication the HISP policy requirements) stated in Section 4. The **Iterations** are indicated by adding a letter subscript to the section number for a security functional component (e.g., 5.2.3(a)). The **Assignment** and **Selection** operations are indicated through italicized texts and **Refinements** through bold texts.

5.1 Identification and Authentication (FIA)

5.1.1 *User Authentication before any action*

5.1.1.1 FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2 Unforgeable authentication

5.1.2.1 FIA_UAU.3.1 The TSF shall *detect* use of authentication data that has been forged by any user of the TSF.

5.1.2.2 FIA_UAU.3.2 The TSF shall *detect* use of authentication data that has been copied from any other user of the TSF.

5.1.3 Multiple Authentication Mechanisms

5.1.3.1 FIA_UAU.5.1 The TSF shall provide the following authentication mechanisms to support user authentication: smart cards authenticator or certificate servers.

5.1.3.2 FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:

For remote logins over untrusted paths (e.g., internet connection provided by an ISP) the TSF shall employ (support) one of the following mechanisms:

- Smart card type authenticator where a remote user is validated by verifying the correctness of a random number generated by the user's smart card.
- Verification of digital certificates issued by a Trusted Certificate Authority (CA)
- Verification of digital certificates through the use of locally maintained Certificate Servers.

5.1.4 User Identification before any action

5.1.4.1 FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of the user.

5.2 Cryptographic Services (FCS)

5.2.1 Cryptographic Key Generation

5.2.1.1(a) FCS_CKM.1.1 The TSF shall generate *public/private* cryptographic keys *used for authentication, digital signatures & encryption key exchange* in accordance with *RC4 key generation algorithm within a RC4 public key crypto algorithm* with a minimum key size of *1024 bits* that meet the requirements in *PKCS#1, X9.30 & X9.31* standards.

5.2.1.1(b) FCS_CKM.1.1 The TSF shall generate *symmetric* cryptographic keys *used for message encryption* in accordance with *Triple DES key generation algorithm within a Triple DES crypto algorithm* with a minimum key size of *56 bits for each stage (or 112 bit equivalent)* that meet the requirements in *X9.52 (FIPS 46-3)* standard.

5.2.2 Cryptographic Key Distribution

5.2.2.1(a) FCS_CKM.2.1 The TSF shall distribute *public* cryptographic keys in accordance with a *Public Key Infrastructure (PKI) using digital certificates* that meets the X.509 standard.

5.2.2.1(b) FCS_CKM.2.1 The TSF shall distribute *symmetric* cryptographic keys in accordance with *RSA key transport* that meets *PKCS#1* & *X9.30* standards.

5.2.3 Cryptographic Operation

5.2.3.1(a) FCS_COP.1.1 The TSF shall perform *2-way Authentication , Symmetric Key Encryption and digital signatures for transmitting HCFA-sensitive transactional messages to a remote TSF*, using *RC4 public key crypto algorithm* with a minimum key size of *1024 bits* that meet the requirements in *PKCS#1, X9.30 & X9.31* standards.

5.2.3.1(b) FCS_COP.1.1 The TSF shall perform *data encryption and digital signatures for transmitting e-mail messages containing HCFA-sensitive information to a remote mail system* using *RC4 public key crypto algorithm* with a minimum key size of *1024 bits* that meet the requirements in *PKCS#1, X9.30 & X9.31* standards.

5.2.3.1(c) FCS_COP.1.1 The cryptographic engine for performing the cryptographic operations specified in 5.23(a) or 5.2.3(b) can either be located in a software or in a hardware crypto module like smartcard.

5.2.3.1(d) FCS_COP.1.1 The TSF shall perform *data encryption/decryption for HCFA-sensitive transactional messages* using *Triple DES crypto algorithm* with a minimum key size of *56 bits for each stage (or 112 bit equivalent)* that meet the requirements in *X9.52 (FIPS 46-3)* standard.

5.3 Trusted Path/Channels (FTP)

5.3.1 Inter-TSF trusted channel

5.3.1.1 FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product (e.g., a web application, mail server) that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

5.3.1.2 FTP_ITC.1.2 The *TSF in an application system generating HCFA-sensitive transactional message or the TSF mail client sending HCFA-sensitive data* should be capable initiating communication via the trusted channel *with its corresponding component in the remote IT product*.

5.3.1.3(a) FTP_ITC.1.3 The TSF in an application system generating HCFA-sensitive transactional message should be capable of using SSL V3.0 protocol with a Public Key Infrastructure (PKI) that supports X.509V3 digital certificates.

5.3.1.3(b) FTP_ITC.1.3 The TSF in a mail system that carries HCFA-sensitive information should be capable of using S/MIME V2.0 protocol with a Public Key Infrastructure (PKI) that supports X.509 V3 digital certificates.

5.4 Security Management (FMT)

5.4.1 Management of Security Functions

5.4.1.1 FMT_MOF.1.1. The TSF shall restrict the ability to determine the behavior of, enable, disable and modify the behavior of the following functions to authorized administrators.

- (a) Functions related to management of digital certificates:
 - (i) Install and Uninstall digital certificates
 - (ii) Query on status of certificate request;
 - (iii) Certificate and CRL retrieval;
 - (iv) Request Certificate revocation.
- (b) Install and Uninstall encryption software
- (c) Install and Uninstall digital signature software
- (d) Generate, store & destroy symmetric keys and Public key/Private key pairs

5.4.2 Management of Security Data

5.4.2.1(a) FMT_MTD.1.1 (User Private Key Storage Management) The TSF shall restrict the ability to *store, retrieve and destroy the user private key (associated with the user public key of a user digital certificate)* to the holder of digital certificate.

5.4.2.1(b) FMT_MTD.1.1 (Server Private Key & Server Digital Certificate Storage Management) The TSF shall restrict the ability to: *(a) store, retrieve and destroy the server private key (associated with the server public key of the server digital certificate) and (b) install and delete the server's digital certificate* to the server's authorized administrator.

5.4.2.1(c) FMT_MTD.1.1 (User Digital Certificate Storage Management) The TSF shall restrict the ability to *install and delete user digital certificate in a directory server (e.g., LDAP)* to the server's authorized administrator.

5.4.2.2 FMT_MTD.1.1 The TSF in STS-HCFA shall enable the holder of user digital certificate to store his/her private key in a secure directory under the control of file system of the user's workstation or offline in a smart card or PCMCIA card.

5.5 Security Audit (FAU)

5.5.1 Audit Data Generation

5.5.1.1 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- (a) start-up and shutdown of the audit functions
- (b) All auditable events for the *basic* level of audit.
- (c) The following specific events:
 - (i) All events relating to management of security functions (section 5.4.1)
 - (ii) User Login events
 - (iii) Events relating to transmission and receipt of specific HCFA-sensitive transactional messages

5.5.1.2 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- (a) Date and time of event, type of event, subject identity, and the outcome (success or failure) of the event; and
- (b) For each audit event type, based on the auditable event definitions of the functional components included in this Functional Package, additional audit event relevant information (e.g., capture of EDI form# in the audit event relating to transmission and receipt of specific HCFA-sensitive transactional messages (refer (c-iii) under 5.5.1.1 above)).

5.5.1.3 FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.5.2 Audit Review

5.5.2.1 FAU_SAR.1.1 The TSF shall provide *system administrators of STS-HCFA* the ability to read the *following information* from the audit records.

- (a) The date, time, and the IP address of the machine from which a HCFA transactional message was transmitted.
- (b) The message ID and the EDI form that was used for the message.
- (c) The destination IP address/ e-mail address to which the message was sent.
- (d) The encryption and signature algorithm that was used for the message
- (e) Any acknowledgement information for the transmitted message.

5.5.3 Restricted Audit Review

5.5.3.1 FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.5.4 *Selectable Audit Review*

5.5.4.1 FAU_SAR.3.1 The TSF shall provide the ability to perform searching & sorting of audit data based on the following:

- (a) All the HCFA transactional messages transmitted/received within a specific time period (based on the date/time fields in the audit records).
- (b) All the HCFA transactional messages of a particular category (e.g., based on EDI form #s) sent in a given time period.
- (c) All the HCFA transactional messages sent to/from a particular location or IP Address.

5.5.5 *Protected Audit Trail Storage*

5.5.5.1 FAU_STG1.1 The TSF shall protect the stored audit records from unauthorized deletion.

5.5.5.2 FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit records.

5.6 Protection of TOE Security Functions (FPT)

5.6.1 *Reliable Time Stamps*

5.6.1.1 FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6 Rationale for choice of ISO 15408 Security Functional classes

The HCFA Internet Security Policy was formulated to regulate the use of internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information as long as “an acceptable method of encryption is utilized to provide for confidentiality and integrity of this data and that authentication or identification procedures are employed”. Hence the security services that are required for STS-HCFA systems are (a) Identification & Authentication (b) Cryptographic services (for providing confidentiality by encrypting messages and providing integrity through digital signatures) and (c) establishment of trusted communication channels between the communicating partners. These services are provided by the following ISO 15408 security functional requirements classes:

- (a) FIA – Identification & Authentication
- (b) FCS – Cryptographic Services
- (c) FTP – Trusted Path/Channels

Hence components from these services were selected to specify the security functional requirements for STS-HCFA. For supporting these services, certain basic security management functions have to be performed and audit data pertaining to security management and user events have to be maintained. The functional requirements needed

for security management and audit management are provided through components from the following classes:

- (a) FMT – Security Management
- (b) FAU - Security Audit

In addition to support the generation and review of audit records, it is necessary that the security functions in STS-HCFA generate time stamps. Hence a component for generating time stamps is chosen from the following family:

FPT – Protection of the TOE security functions

This Functional Package does not deal with the following:

- (a) Access Control to the data repository which contains the information needed to generate HCFA sensitive messages.
- (b) Access Control to the functions necessary to generate/receive HCFA sensitive messages.
- (c) Security mechanisms needed for network perimeter defense like configuration of firewalls, routers etc.,

The exact mappings between: (a) the identified threats/HCFA Internet Security Policy components, (b) the security objectives formulated to counter these threats and support the HCFA Internet Security Policy requirements and (c) the exact ISO/IEC 15408 security functional requirements components to meet these objectives are given in a table in Appendix A.

Appendix A

Mappings between Policies/Threats, Security Objectives & Security Functional Components

Policy Component/Threat	Security Objective	ISO/IEC 15408 Security Functional Requirement Component
P.CHANNEL	O.CHANNEL	FTP_ITC.1.1 (5.3.1.1) FTP_ITC.1.2 (5.3.1.2) FTP_ITC.1.3 (5.3.1.3(a) & (b))
T.ENTRY T.SPOOF P.AUTHENTICATE	O.AUTHENTICATE	FIA_UAU.2.1 (5.1.1.1) FIA_UAU.3.1 (5.1.2.1) FIA_UAU.3.2 (5.1.2.2) FIA_UAU.5.1 (5.1.3.1) FIA_UAU.5.2 (5.1.3.2) FIA_UID.2.1 (5.1.4.1) FCS_COP.1.1 (5.2.3.1(b))
T.SNIFF T.INTEGRITY P.SENSITIVE P.SCOPE P.ENCRYPT	O.ENCRYPT O.INTEGRITY	FCS_CKM.1.1 (5.2.1.1(a) & (b)) FCS_CKM.2.1 (5.2.2.1(a) & (b)) FCS_COP.1.1 (5.2.3.1(a), (b), (c) & (d))
P.SECMGT	O.SECADMIN	FMT_MOF.1.1 (5.4.1.1) FMT_MTD.1.1 (5.4.2.1 (a), (b) & (c) and 5.4.2.2)
P.ACCOUNTABILITY	O.AUDIT	FAU_GEN.1.1 (5.5.1.1) FAU_GEN.1.2 (5.5.1.2) FAU_GEN.2.1 (5.5.1.3) FAU_SAR.1.1 (5.5.2.1) FAU_SAR.2.1 (5.5.3.1) FAU_SAR.3.1 (5.5.4.1) FAU_STG.1.1 (5.5.5.1) FAU_STG.1.2 (5.5.5.2) FPT_STM.1.1 (5.6.1.1)

GLOSSARY OF TERMS

ISO/IEC 15408 – Security Criteria related

- ISO - International Organization for Standardization**
- IEC - International Electrotechnical Commission**
- TOE - Target of Evaluation – the Information System for which Security requirements are to be stated and evaluated for Conformance to those requirements**
- TSF - TOE Security Functions – the functions within the information System under evaluation which provide all security relevant Functions.**
- PP - Protection Profile – A construct or framework used for stating Security functional requirements and Security assurance Requirements for a product or system – reflects statement Of user security needs**
- ST - Security Target – A construct or framework used for stating the Security mechanisms in a product or system so as to claim Conformance to a given PP or stated set of security standards – Reflects vendor’s claims of conformance to a PP used by a user Community or adherence to accepted standards.**
- FP - Functional Package – A collection of security functional Requirements relating to an organization’s security policy or Security interface standard**

Abbreviations related to HCFA Internet Security Policy

- HISP - HCFA Internet Security Policy**
- STS-HCFA – Systems generating and transmitting HCFA Privacy-Act Protected and/or sensitive HCFA information**

Bibliography

[HISP] – HCFA INTERNET SECURITY POLICY

(<http://www.hcfa.gov/security/iseclpky.htm>)

[ISO/IEC 15408-1] Evaluation Criteria for IT Security – Part 1: Introduction and General Model

(<http://csrc.nist.gov/cc/ccv20/15408-1.pdf>)

[ISO/IEC 15408-2] Evaluation Criteria for IT Security – Part 2: Security Functional Requirements

(<http://csrc.nist.gov/cc/ccv20/15408-2.pdf>)

[ISO/IEC 15408-3] Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements

(<http://csrc.nist.gov/cc/ccv20/15408-3.pdf>)